BUNDESREPUBLIK DEUTSCHLAND

CERTIFIED COPY OF PRIORITY DOCUMENT

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	199 58 004.9
Anmeldetag:	2. Dezember 1999
Anmelder/Inhaber:	Philips Corporate Intellectual Property GmbH, Hamburg/DE
Bezeichnung:	Drahtloses Netzwerk mit einer Prozedur zur Schlüsseländerung
IPC:	H 04 Q, H 04 L, H 04 B

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 7. August 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Seiler

A 9161
03/00
EDV-L

ZUSAMMENFASSUNG

Drahtloses Netzwerk mit einer Prozedur zur Schlüsseländerung

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten vorgesehen sind und die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten vorgesehen sind. Erfindungsgemäß sendet die Funknetzwerk-Steuerung ein mit einem alten Schlüssel verschlüsselten Schlüsseländerungsbefehl an ein Terminal. Als Antwort sendet das Terminal ein mit einem neuen Schlüssel verschlüsselten Schlüsselbestätigungsbefehls an die Funknetzwerk-Steuerung.

Fig. 4

BESCHREIBUNG

Drahtloses Netzwerk mit einer Prozedur zur Schlüsseländerung

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten vorgesehen sind und die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten vorgesehen sind.

Aus dem Buch „The GSM System for Mobile Communications" von Michel Mouly und Marie-Bernadette Pautet, Verlag Cell & Sys, 1992, Seiten 391 bis 395, ist bekannt, dass Daten zwischen einer Basisstation und einem Terminal verschlüsselt übertragen werden. Der für die Übertragung benötigte Schlüssel wird in bestimmten Zeitabständen verändert. Hierfür ist eine Prozedur in drei Schritten vorgesehen.

Der Erfindung liegt die Aufgabe zugrunde, ein drahtloses Netzwerk zu schaffen, das eine andere Prozedur zur Änderung eines Schlüssels angibt.

Die Aufgabe wird durch ein drahtloses Netzwerk der eingangs genannten Art dadurch gelöst,
dass die Funknetzwerk-Steuerung zur Sendung eines mit einem alten Schlüssel verschlüsselten Schlüsseländerungsbefehl an ein Terminal vorgesehen ist und
dass das Terminal zur Sendung eines mit einem neuen Schlüssel verschlüsselten Schlüsselbestätigungsbefehls an die Funknetzwerk-Steuerung vorgesehen ist.

Unter dem erfindungsgemäßen drahtlosen Netzwerk ist ein Netzwerk mit mehreren Funkzellen zu verstehen, in denen jeweils eine Basisstation und mehrere Terminals Steuer- und Nutzdaten drahtlos übertragen. Eine drahtlose Übertragung dient zur Übertragung von Informationen z.B. über Funk-, Ultraschall- oder Infrarotwege.

Erfindungsgemäß bestätigt ein Terminal einen mit einem neuen Schlüssel verschlüsselten Schlüsseländerungsbefehl mit der Sendung eines mit dem neuen Schlüssel verschlüsselten

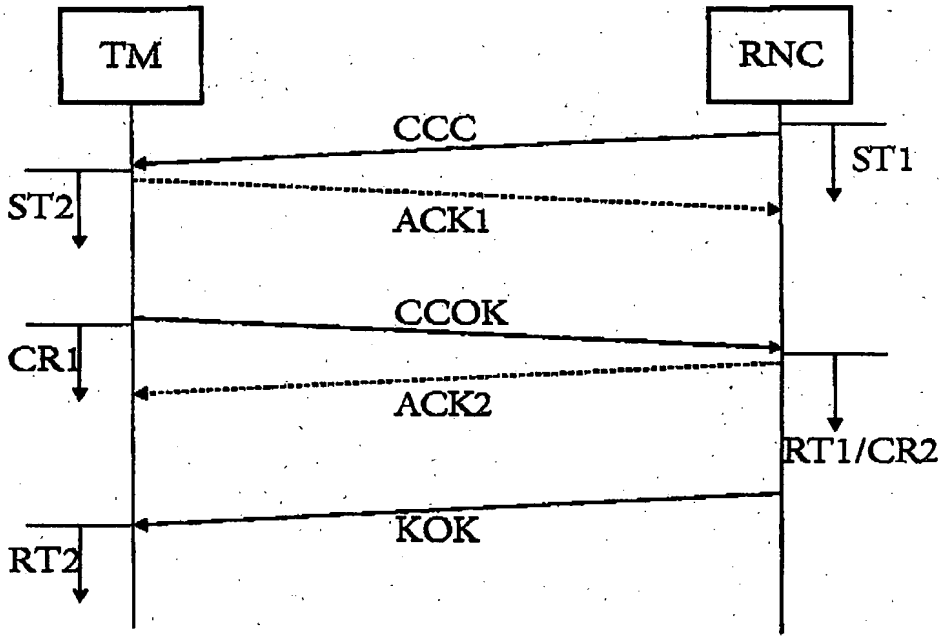

FIG. 4

Schlüsselbestätigungsbefehl. Wenn dem Terminal der neue Schlüssel fehlerhaft bekannt gemacht worden ist, kann kein Schlüsselbestätigungsbefehl detektiert werden. Somit kann der neue Schlüssel nicht verwendet werden.

Ausführungsbeispiele der Erfindung werden nachstehend anhand der Fig. näher erläutert. Es zeigen:

Fig. 1	ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren Terminals,
Fig. 2	ein Schichtenmodell zur Erläuterung verschiedener Funktionen eines Terminals oder einer Funknetzwerk-Steuerung,
Fig. 3	ein Blockschaltbild zur Erläuterung des Verschlüsselungsmechanismus in einem Terminal oder einer Funknetzwerk-Steuerung und
Fig. 4	einen Ablauf verschiedener Befehle bei einer Änderungsprozedur des für die Verschlüsselung benötigten Schlüssels.

In Fig. 1 ist ein drahtloses Netzwerk, z.B. Funknetzwerk, mit einer Funknetzwerk-Steuerung (Radio Network Controller = RNC) 1 und mehreren Terminals 2 bis 9 dargestellt. Die Funknetzwerk-Steuerung 1 ist für Steuerung aller am Funkverkehr beteiligten Komponenten verantwortlich, wie z.B. der Terminals 2 bis 9. Ein Steuer- und Nutzdatenaustausch findet zumindest zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 statt. Die Funknetzwerk-Steuerung 1 baut jeweils eine Verbindung zur Übertragung von Nutzdaten auf.

In der Regel sind die Terminals 2 bis 9 Mobilstationen und die Funknetzwerk-Steuerung 1 ist fest installiert. Eine Funknetzwerk-Steuerung 1 kann gegebenenfalls aber auch beweglich bzw. mobil sein.

In dem drahtlosen Netzwerk werden beispielsweise Funksignale nach dem FDMA-, TDMA- oder CDMA-Verfahren (FDMA = frequency division multiplex access, TDMA = time division multiplex access, CDMA = code division multiplex access) oder nach einer Kombination der Verfahren übertragen.

Beim CDMA-Verfahren, das ein spezielles Code-Spreiz-Verfahren (code spreading) ist, wird eine von einem Anwender stammende Binärinformation (Datensignal) mit jeweils einer unterschiedlichen Codesequenz moduliert. Eine solche Codesequenz besteht aus einem pseudo-zufälligen Rechtecksignal (pseudo noise code), dessen Rate, auch Chiprate genannt, in der Regel wesentlich höher als die der Binärinformation ist. Die Dauer eines Rechteckimpulses des pseudo-zufälligen Rechtecksignals wird als Chipintervall T_C bezeichnet. $1/T_C$ ist die Chiprate. Die Multiplikation bzw. Modulation des Datensignals mit dem pseudo-zufälligen Rechtecksignal hat eine Spreizung des Spektrums um den Spreizungsfaktor $N_C = T/T_C$ zur Folge, wobei T die Dauer eines Rechteckimpulses des Datensignals ist.

Nutzdaten und Steuerdaten zwischen wenigstens einem Terminal (2 bis 9) und der Funknetzwerk-Steuerung 1 werden über von der Funknetzwerk-Steuerung 1 vorgegebene Kanäle übertragen. Ein Kanal ist durch einen Frequenzbereich, einen Zeitbereich und z.B. beim CDMA-Verfahren durch einen Spreizungscode bestimmt. Die Funkverbindung von der Funknetzwerk-Steuerung 1 zu den Terminals 2 bis 9 wird als Downlink und von den Terminals zur Basisstation als Uplink bezeichnet. Somit werden über Downlink-Kanäle Daten von der Basisstation zu den Terminals und über Uplink-Kanäle Daten von Terminals zur Basisstation gesendet.

Beispielsweise kann ein Downlink-Steuerkanal vorgesehen sein, der benutzt wird, um von der Funknetzwerk-Steuerung 1 Steuerdaten vor einem Verbindungsaufbau an alle Terminals 2 bis 9 zu verteilen. Ein solcher Kanal wird als Downlink-Verteil-Steuerkanal (broadcast control channel) bezeichnet. Zur Übertragung von Steuerdaten vor einem Verbindungsaufbau von einem Terminal 2 bis 9 zur Funknetzwerk-Steuerung 1 kann beispielsweise ein von der Funknetzwerk-Steuerung 1 zugewiesener Uplink-Steuerkanal verwendet werden, auf den aber auch andere Terminals 2 bis 9 zugreifen können. Ein Uplink-Kanal, der von mehreren oder allen Terminals 2 bis 9 benutzt werden kann, wird als gemeinsamer Uplink-Kanal (common uplink channel) bezeichnet. Nach einem Verbindungsaufbau z.B. zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1 werden Nutzdaten über einen Downlink- und ein Uplink-Nutzkanal übertragen. Kanäle,

die nur zwischen einem Sender und einem Empfänger aufgebaut werden, werden als dedizierte Kanäle bezeichnet. In der Regel ist ein Nutzkanal ein dedizierter Kanal, der von einem dedizierten Steuerkanal zur Übertragung von verbindungsspezifischen Steuerdaten begleitet werden kann.

Zur Einbindung eines Terminals 2 bis 9 zu einer Funknetzwerk-Steuerung 1 ist ein kollisionsbehafteter Kanal zuständig, der im folgenden als signalisierter RACH-Kanal (RACH = Random Access Channel) bezeichnet wird. Über einen solchen signalisierten RACH-Kanal können auch Datenpakete übertragen werden.

Damit Nutzdaten zwischen der Funknetzwerk-Steuerung 1 und einem Terminal ausgetauscht werden können, ist es erforderlich, dass ein Terminal 2 bis 9 mit der Funknetzwerk-Steuerung 1 synchronisiert wird. Beispielsweise ist aus dem GSM-System (GSM = Global System for Mobile communication) bekannt, in welchem eine Kombination aus FDMA- und TDMA-Verfahren benutzt wird, dass nach der Bestimmung eines geeigneten Frequenzbereichs anhand vorgegebener Parameter die zeitliche Position eines Rahmens bestimmt wird (Rahmensynchronisation), mit dessen Hilfe die zeitliche Abfolge zur Übertragung von Daten erfolgt. Ein solcher Rahmen ist immer für die Datensynchronisation von Terminals und Basisstation bei TDMA-, FDMA- und CDMA-Verfahren notwendig. Ein solcher Rahmen kann verschiedene Unter- oder Subrahmen enthalten oder mit mehreren anderen aufeinanderfolgenden Rahmen einen Superrahmen bilden. Aus Vereinfachungsgründen wird im folgenden von einem Rahmen ausgegangen, der als Referenzrahmen bezeichnet wird.

Die Steuer- und Nutzdatenaustausch über die Funkschnittstelle zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 kann mit dem in Fig. 2 dargestellten, beispielhaften Schichtenmodell oder Protokollarchitektur (vgl. z.B. 3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) RAN; Working Group 2 (WG2); Radio Interface Protocol Architecture; TS 25.301 V3.2.0 (1999-10)) erläutert werden. Das Schichtenmodell besteht aus drei Protokollschichten: der physikalischen Schicht PHY, der Datenverbindungsschicht mit den Unterschichten MAC und RLC (in Fig. 2 sind mehrere Ausprägungen der Unterschicht RLC dargestellt) und der Schicht RRC. Die Unterschicht

MAC ist für die Medienzugriffssteuerung (Medium Access Control), die Unterschicht RLC für die Funkverbindungssteuerung (Radio Link Control) und die Schicht RRC für die Funkverwaltungssteuerung (Radio Resource Control) zuständig. Die Schicht RRC ist für die Signalisierung zwischen den Terminals 2 bis 9 und der Funknetzwerk-Steuerung 1 verantwortlich. Die Unterschicht RLC dient zur Steuerung einer Funkverbindung zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1. Die Schicht RRC steuert die Schichten MAC und PHY über Steuerungsverbindungen 10 und 11. Hiermit kann die Schicht RRC die Konfiguration der Schichten MAC und PHY steuern. Die physikalische Schicht PHY bietet der MAC-Schicht Transportverbindungen 12 an. Die MAC-Schicht stellt der RLC-Schicht logische Verbindungen 13 zur Verfügung. Die RLC-Schicht ist über Zugangspunkte 14 von Applikationen erreichbar.

Bei einem solchen drahtlosen Netzwerk werden die Daten aus Sicherheits- und Vertraulichkeitsgründen verschlüsselt über die Funkschnittstelle übertragen, um eine Abhören der Daten zu verhindern. Die Verschlüsselung wird in der Datenverbindungsschicht (z. B. in der RLC- oder MAC-Schicht) durchgeführt. Wie Fig. 3 zeigt, werden die Daten D über eine Exklusiv-Oder-Funktion (XOR) mit einer Verschlüsselungsmaske M verknüpft, so dass sich ein verschlüsselter Datenstrom C_D ergibt. Die Verschlüsselungsmaske M wird in einer Verschlüsselungs-Funktion 16 gebildet, die nach einem Verschlüsselungs-Algorithmus arbeitet und als Eingangswerte den Schlüssel CK und andere hier nicht näher dargestellte Parameter P erhält.

Der Schlüssel muss sowohl der Funknetzwerk-Steuerung 1 als auch den Terminals 2 bis 9 bekannt sein. Dieser Schlüssel wird zu bestimmten Zeitpunkten geändert (z.B. alle 2 Stunden). Das Terminal erhält die Information über den neuen Schlüssel in einer separaten hier nicht näher dargestellten Datenaustauschprozedur. Hierbei wird vermieden, dass der Schlüssel selbst über die Funkschnittstelle übertragen wird. Mit einer speziellen Prozedur CKCS (cipher key change synchronisation), die als Schlüsseländerungssynchronisations-Prozedur bezeichnet wird, wird dann ein synchronisiertes Umschalten vom alten auf den neuen Schlüssel zwischen Terminal und Funknetzwerk-Steuerung 1 durchgeführt. Zuerst wird von der Funknetzwerk-Steuerung 1 (vgl. Fig. 4) jede Übertragung von Daten zu dem Terminal (Downlink), welche verschlüsselt werden

sollen, gestoppt (ST1). Die einzige Ausnahme ist ein im folgenden beschriebener Schlüsseländerungsbefehl CCC. Empfangene Uplink-Daten werden weiterhin mit dem bisherigen Schlüssel entschlüsselt. Dann wird von der Funknetzwerk-Steuerung 1 dem Terminal ein Schlüsseländerungsbefehl CCC (verschlüsselt mit dem alten Schlüssel) über einen Signalisierungskanal gesendet. Aus Sicherheitsgründen ist es unerheblich, ob Daten, die vor der Prozedur CKCS mit dem alten Schlüssel verschlüsselt übertragen wurden, aber unquittiert (keine Bestätigung) blieben, nach der Prozedur CKCS bei erneuter Übertragung nun mit dem neuen Schlüssel verschlüsselt werden.

Nachdem das Terminal den Schlüsseländerungsbefehl CCC erhalten hat, wird nur ein Bestätigungsbefehl ACK1 zur Funknetzwerk-Steuerung 1 gesendet, damit die Funknetzwerk-Steuerung 1 nicht nach einer bestimmten Zeit den Schlüsseländerungsbefehl CCC erneut sendet. Jede Übertragung von Daten (Uplink), welche verschlüsselt werden sollen, werden von dem Terminal ebenfalls gestoppt (ST2). Die einzige Ausnahme ist ein im folgenden beschriebener Schlüsselbestätigungsbefehl CCOK, der mit dem neuen Schlüssel verschlüsselt wird. Das Terminal ist nach Sendung des Schlüsselbestätigungsbefehls CCOK bereit, Daten sowohl mit dem alten als auch mit dem neuen Schlüssel zu empfangen und zu entschlüsseln (CR1). Die Funknetzwerk-Steuerung 1 ist nach dem Absenden des Schlüsseländerungsbefehls CCC und dem Empfang der Bestätigungsnachricht ACK1 bereit. Daten sowohl mit dem neuen als auch mit dem alten Schlüssel zu entschlüsseln. Nach Empfang von ACK1 erwartet die Funknetzwerk-Steuerung 1 nur den Schlüsselbestätigungsbefehl CCOK, der mit dem neuen Schlüssel verschlüsselt wurde. Ergibt die Entschlüsselung dieses Befehls in der Funknetzwerk-Steuerung 1 keinen sinnvollen Inhalt (d.h. die Funknetzwerk-Steuerung kann nicht zweifelsfrei erkennen, dass es sich um den Befehl CCOK handelt), weil das Terminal einen fehlerhaften neuen Schlüssel für die Verschlüsselung verwendet hat, kann die Funknetzwerk-Steuerung 1 erkennen, dass dem Terminal ein fehlerhafter neuer Schlüssel bekannt gemacht wurde. Die Entschlüsselung dieses Befehls CCOK mit dem alten Schlüssel ergibt ebenfalls keinen sinnvollen Inhalt. Durch dieses zweite fehlerhafte Verschlüsselungsergebnis gewinnt die Funknetzwerk-Steuerung noch zusätzliche Gewissheit, dass dem Terminal ein fehlerhafter neuer Schlüssel bekannt ist.

Der Empfang des Schlüsselbestätigungsbefehls CCOK wird von der Funknetzwerk-Steuerung 1 mit einem Bestätigungsbefehl ACK2 dem Terminal gemeldet. Ergab die Entschlüsselung von CCOK mit dem neuen Schlüssel, dass CCOK empfangen wurde, so nimmt die Funknetzwerk-Steuerung 1 die Datenübertragung (Downlink) zum Terminal mit dem neuen Schlüssel wieder auf (RT1). Empfangene Daten werden nur noch mit dem neuen Schlüssel demaskiert. Die Funknetzwerk-Steuerung 1 sendet dann einen Übereinstimmungsbefehl KOK zum Terminal, der mit dem neuen Schlüssel verschlüsselt ist.

Konnte kein Schlüsselbestätigungsbefehl CCOK entschlüsselt werden (wie oben beschrieben), wird wieder nur noch der alte Schlüssel sowohl zum Empfang als auch zum Senden verwendet (RT1/CR2). Die Funknetzwerk-Steuerung 1 sendet dann einen Übereinstimmungsbefehl KOK zum Terminal, der mit dem alten Schlüssel verschlüsselt ist. Danach nimmt die Funknetzwerk-Steuerung 1 wieder das Senden von anderer Daten, falls vorhanden, auf.

Damit ein Schlüsselwechsel mit einem Terminal und Funknetzwerk-Steuerung bekannten neuen Schlüssel noch möglich wird, muss die RLC-Schicht eine hier nicht näher beschriebene, für die Datenaustauschprozedur verantwortliche Management-Schicht informieren, dass ein anderer neuer Schlüssel dem Terminal mitgeteilt werden muss.

Nach Empfang dieses Übereinstimmungsbefehls KOK, der mit dem neuen Schlüssel verschlüsselt wurde, nimmt das Terminal die Datenübertragung (Uplink) mit dem neuen Schlüssel auf (RT2). Hiermit ist die Prozedur CKCS abgeschlossen und somit wird die Datenübertragung nur mit diesem Schlüssel durchgeführt.

Nach Empfang dieses Übereinstimmungsbefehls KOK, der mit dem alten Schlüssel verschlüsselt wurde, nimmt das Terminal die Datenübertragung (Uplink) mit dem alten Schlüssel wieder auf (RT2) und der gleichzeitige Empfang mit dem neuen Schlüssel wird beendet. Hiermit ist die Prozedur CKCS abgebrochen und somit auch beendet.

Dadurch, dass das Terminal zwischen CR1 und RT2 empfangene Daten sowohl mit dem

alten als auch mit dem neuen Schlüssel entschlüsselt, kann das Terminal erkennen, ob die Prozedur CKC erfolgreich abgeschlossen wurde (dann empfängt das Terminal den Übereinstimmungsbefehl KOK verschlüsselt mit dem neuen Schlüssel und die Entschlüsselung mit dem neuen Schlüssel ergibt, dass KOK geschickt wurde, während die Entschlüsselung mit dem alten Schlüssel keinen sinnvollen Inhalt ergibt) oder ob die Prozedur nach dem Austausch eines neuen Schlüssels erneut begonnen werden muss (dann empfängt das Terminal den mit dem alten Schlüssel verschlüsselten Übereinstimmungsbefehl KOK: hier ergibt die Entschlüsselung mit dem neuen Schlüssel keinen sinnvollen Inhalt, während die Entschlüsselung mit dem alten Schlüssel ergibt, dass KOK geschickt wurde). Dadurch wird vermieden, dass infolge eines vom Terminal fehlerhaft empfangenen Schlüssels alle Verbindungen zwischen Terminal und Netzwerk abbrechen.

Die beschriebene Prozedur CKCS bezieht sich zunächst nur auf die Signalisierungsverbindung. Datenverbindungen, die ebenfalls mit Übertragungswiederholungen arbeiten, werden in die Prozedur einbezogen, indem ihren jeweiligen Schichten RLC ebenfalls ein Stoppbefehl (Terminal: ST2, Netzwerk ST1) bzw. ein Befehl zur Wiederaufnahme der Übertragung von Nutzdaten mitgeteilt wird (Terminal: RT2, Netzwerk: RT1/CR2).

PATENTANSPRÜCHE

1. Drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten vorgesehen sind und die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten vorgesehen sind,

dadurch gekennzeichnet,

dass die Funknetzwerk-Steuerung zur Sendung eines mit einem alten Schlüssel verschlüsselten Schlüsseländerungsbefehl an ein Terminal vorgesehen ist und

dass das Terminal zur Sendung eines mit einem neuen Schlüssel verschlüsselten Schlüsselbestätigungsbefehls an die Funknetzwerk-Steuerung vorgesehen ist.

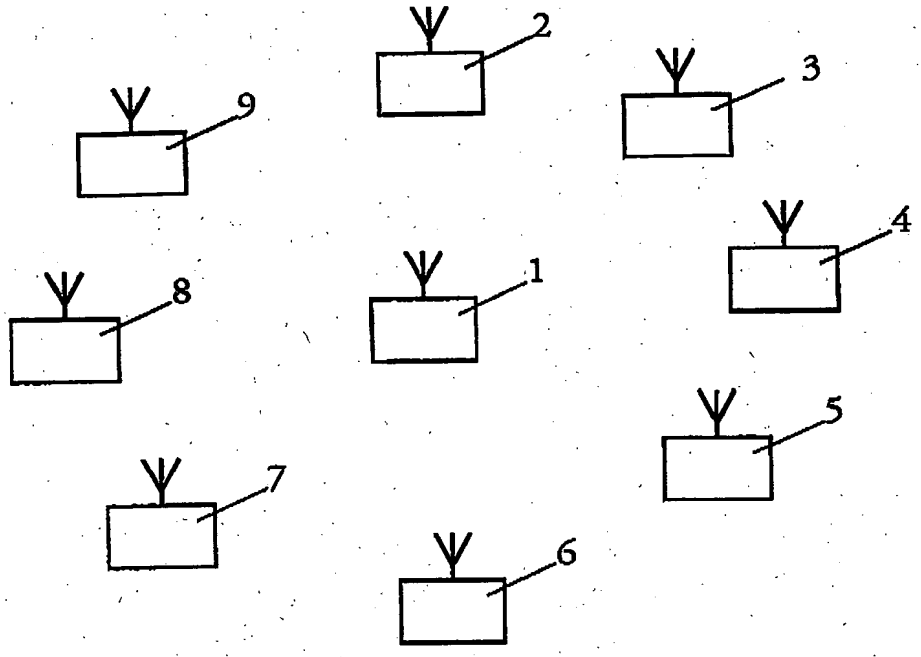

FIG. 1

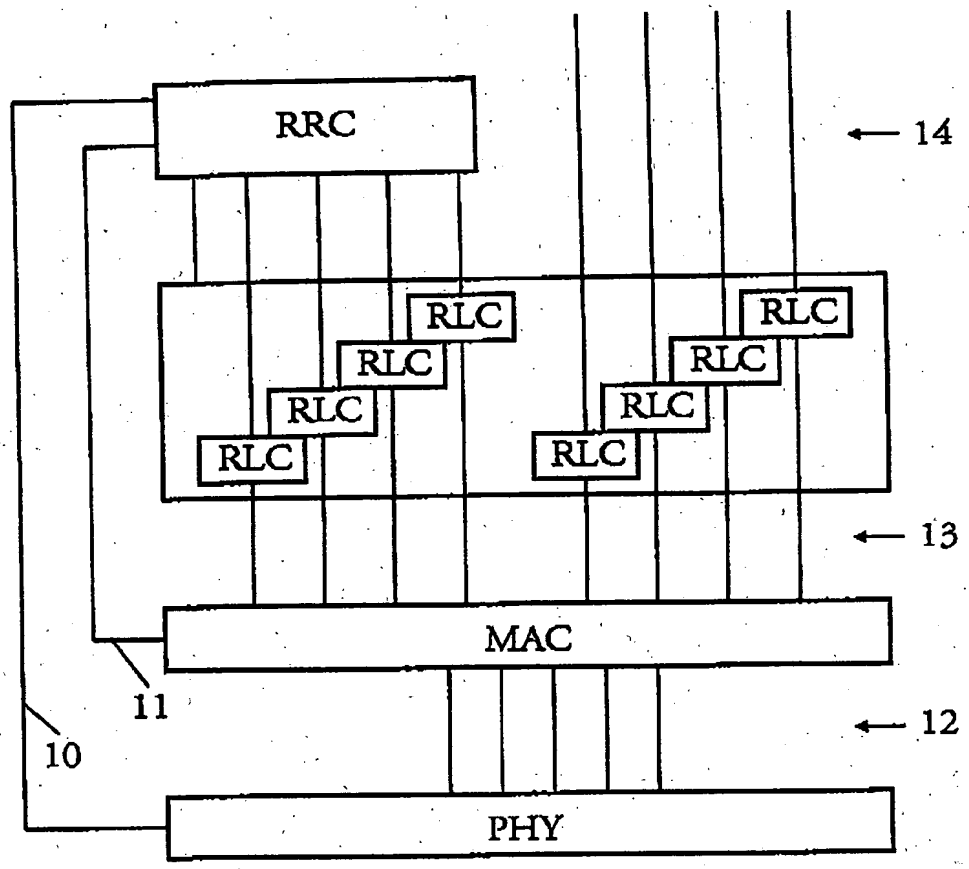

FIG. 2

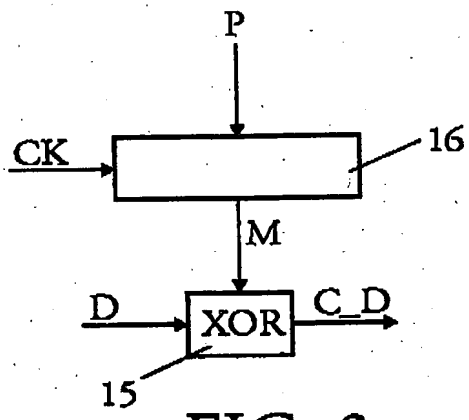
P
CK
16
M
D
XOR
C_D
15

FIG. 3

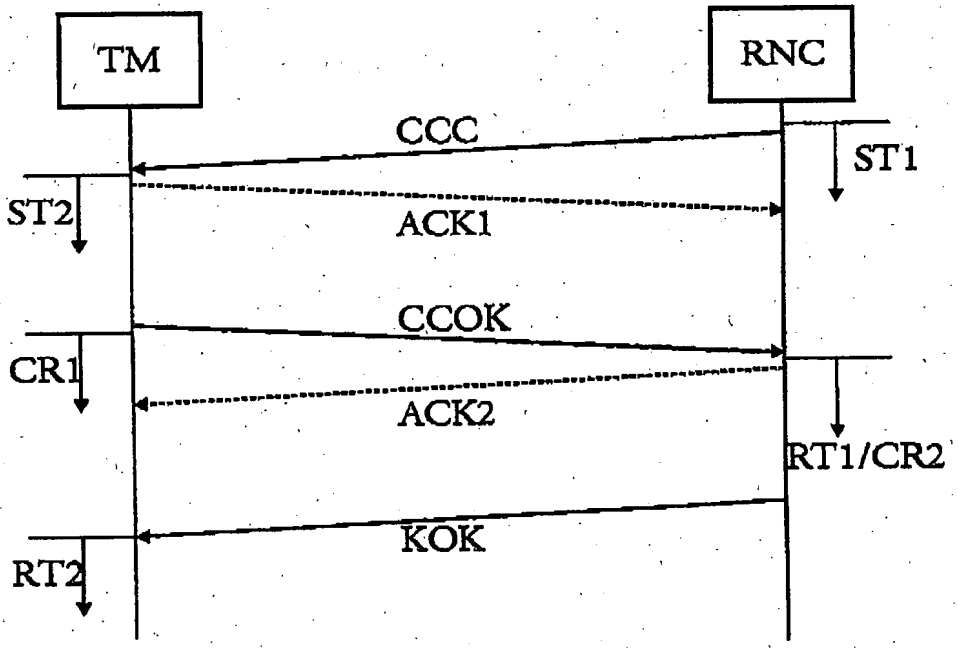
TM
RNC
CCC
ST1
ST2
ACK1
CCOK
CR1
ACK2
RT1/CR2
KOK
RT2

FIG. 4